APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/401,251	09/23/1999	CATHERINE M. KEENE	A0653-1160	4434

7590   07/17/2002

DAVID R. STEVENS
STEVENS & WESTBERG, LLP
99 NORTH FIRST STREET
SUITE 201
SAN JOSE, CA 95113

EXAMINER
PHAM, HUNG Q

ART UNIT	PAPER NUMBER
2172	

DATE MAILED: 07/17/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _27 June 2002_ .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

DETAILED ACTION

1.   The applicants amended claims 1-15 and added claim 16 in the

amendment received on 06/27/2002. The pending claims are 1-16. Applicants'

arguments have been fully considered by the examiner.

2.   Applicant's arguments with respect to claims 1-12 have been considered

but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this Office

action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4.   The changes made to 35 U.S.C. 102(e) by the American Inventors

Protection Act of 1999 (AIPA) do not apply to the examination of this application as the

application being examined was not (1) filed on or after November 29, 2000, or (2)

voluntarily published under 35 U.S.C. 122(b). Therefore, this application is examined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. **Claims 13-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Thorsen [USP 6,052,688].**

Regarding to claim 13, Thorson teaches a computer program product for use with a computer system, *a central processing unit and means coupled to the central processing unit for storing a database to automatically manage objects for viewing and marking an object having varying formats without the use of any originating application of a file to view the object* (FIG. 3B), comprises: *computer readable code means for establishing an object in a storage location* (FIG. 2, col. 8); *computer readable code means for identifying a user to have limited access to information associated with the object* (Col. 11, lines 6-65); *computer readable code means for establishing privilege access criteria that define the scope of access of a version of the object for the user* (Col. 10, line 35-Col. 11, line 5 and Col. 11, lines 27-33); *computer readable code means for receiving an object request by a requestor* (Col. 11, lines 56-65); *computer readable code means for verifying the requestor's user privilege access criteria* (see col. 11, lines 49-60); and *computer readable code means for transmitting a version of the requested object in the form of a redacted document that marks information according to the requestor's user privilege access criteria* (col. 11, line 60-Col. 12, line 17 and Col. 12, lines 50-67).

Regarding to claim 14, Thorsen teaches a computer program product for using

with a data processing and storage system for obtaining a view of a database or a

subset of a database (Col. 20, lines 38-61) and controlling read and write operations by

using access control parameters (Col. 15, lines 18-21). The Thorsen computer program

product comprises: *identifying a user to have access to the object* (Col. 11, lines 6-60);

establishing privilege access criteria that define the scope of access of a version of the object

for the user (Col. 10, line 35-Col. 11, line 5 and Col. 11, lines 27-33); *receiving an object*

request by a requestor (see col. 11, lines 56-65); *verifying the requestor's user privilege*

access criteria (see col. 11, lines 49-60); *transmitting a redacted version of a requested*

object in the form of a document file containing the version of the requested object that was

filtered according to the requestor's user privilege access criteria (col. 11, line 60-Col. 12,

line 17 and Col. 12, lines 50-67).

Regarding to claim 15, Thorsen teaches a computer server having a data base

for storing data pertaining to product information, a method of securely transferring data

between a source and an access destination (Abstract and FIG. 3B) comprises:

establishing an object in a storage location (FIG. 2, col. 8); *identifying a user to have limited*

access to the object (Col. 11, lines 6-60); *establishing privilege access criteria that define the*

scope of access of a version of the object for the user (Col. 10, line 35-Col. 11, line 5 and

Col. 11, lines 27-33); *receiving an object request by a requestor* (Col. 11, lines 56-65);

verifying the requestor's user privilege access criteria (Col. 11, lines 49-60); *setting up a*

version of an object and associated documents according to user access privileges for

transmission to the user; and *transmitting a redacted version of the requested object that set*

up according to the requestor's user privilege access criteria, wherein the access criteria

defines the information in which a user has privileges of access to the version of the requested

object (col. 11, lines 60-Col. 12, lines 17 and Col. 12, lines 50-67).

Regarding to claim 16, Thorsen teaches a system for controlling access to and

associating data in an application independent fashion, which enables data of different

nature to be handled in a conform way by using data access node (Col. 3, lines 9-22) as

an application server having access to a database for storing objects and associated

documents, a method of securely transferring a version of an object and associated

documents from the application server to a user system via a network (FIG. 3B, Col. 4,

lines 16-38) comprises: *establishing privilege access criteria that define the scope of access*

permitted to a user of a version of the object that may be set up and sent to the privileged user

(Col. 10, line 35-Col. 11, line 5 and Col. 11, lines 27-33); *receiving an object request by a*

user via a network for access to a version of an object to which the user has access privileges

(Col. 11, lines 56-65); *verifying the requestor's user privilege access criteria* (Col. 11, lines

49-60); *setting up a version of an object and associated documents according to user access*

privileges for transmission to the user; and *transmitting a version of the requested object that*

was set up according to the requestor's user privilege access criteria in the form of a document

file that includes a version of the requested object and a version of associated documents via

the network (col. 11, lines 60-Col. 12, lines 17 and Col. 12, lines 50-67).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for

all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

7.   This application currently names joint inventors. In considering

patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the

subject matter of the various claims was commonly owned at the time any inventions

covered therein were made absent any evidence to the contrary. Applicant is advised

of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of

each claim that was not commonly owned at the time a later invention was made in

order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35

U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8.   **Claims 1-12 are rejected under 35 U.S.C. 103(a) as being**

unpatentable over Thorsen [USP 6,052,688].

Regarding to claim 1, Thorsen teaches a system for controlling access to and

associating data in an application independent fashion. The Thorsen system enables

data of different nature to be handled in a conform way and for allowing different views

as *the versions* of stored data objects depending on different aspects of the stored

objects or different access rights of a user (Col. 3, lines 9-22). The Thorsen system

comprises: *a database for storing an object and associated information, the object comprising*

distinguishable groups of data, each group or data having associated access criteria for access

to the groups of data (FIG. 3B, Col. 8, lines 43-56). As shown in FIG. 3B, Thorsen

discloses a state of the art database 52, storing data in a number of tables 54 and being

provided with specific data associations. Depending on a control file, the data

associations are rearranged; references or pointers to each of the selected data items

of the tables 54 are arranged and stored in a number of data access nodes 56 as *an*

application server. A client 58, for example an application program, communicates with

the access nodes 56 of the access structure and a new interface is provided between

the old database and the user (Col. 8, lines 42-52). This indicates *an application server*

configured to control access to data stored in the database. As shown in FIG. 8 is a flow

chart for implementing an object access control means or an object filter. The object

filter is used in conjunction with the access control to protect an object referred to by an

access node. In step 124, upon a user command (cmd=dir) all objects are copied to or

listed in an object list 128. Thereafter, in step 132 every object in the object list is

checked in respect of whether or not the user is permitted access to it. An object access

list 134 is thereby used as a check reference. If access right exists for an object, a copy

of or a reference to that object is input in a user list, step 136, and is communicated to

the user in step 138 by call 140 (Col. 11, line 66-Col. 12, line 11). This indicates *the*

application server configured to set up and send a document file having a representation of an

object and associated documents that are stored in the database. Thorsen further disclosed *a*

memory for storing software code for controlling the operation of the application server (FIG.

1, Col. 7, lines 5-16 and Col. 9, lines 31-50) and *access application code stored in the*

memory and executable by the application server (Col. 9, line 1-Col. 10, line 7). As shown

in FIG. 7 as a flow chart of access control, an access node process is started and

initialized in step 72, and access node parameters concerning other nodes and objects

referred to by the node are read from a control file 74. In step 76 the access node is

kept in a waiting condition, waiting for incoming user calls 78. If a user call is received,

the access node process starts a subprocess in step 80 and sets a timer depending on

the control file 82 for the period the subprocess is allowed to exist. In step 84, the

subprocess verifies the user, depending on control file 86 containing information about

accepted and permitted user identities. The address and the identity of the user is

polled in communication 88. If the user is permitted and accepted, the user is logged in

to the access node in step 104 and 106 and is allowed access to functions of the

access node and objects encapsulated in or referred to by the access node. Thereafter,

further access to and communication of data and references contained in the access

node is controlled by means of an access filter having certain access control

parameters and allowing different users different views of the access node, the access

structure and the underlying data. In step 124 of FIG. 8, upon a user command

(cmd=dir) all objects are copied to or listed in an object list 128. Thereafter, in step 132

every object in the object list is checked in respect of whether or not the user is

permitted access to it. An object access list 134 is thereby used as a check reference. If

access right exists for an object, a copy of or a reference to that object is input in a user

list, step 136, and is communicated to the user in step 138 by call 140 (Col. 11, line 34-

Col. 12, line 11). This indicates *the application code being responsive to the access criteria*

associated with the groups of data contained within a version of an object and to

predetermined privileges for allowing controlled access to individual groups of data contained

within the version of an object by an individual user that was set up to be sent to a user

computer system and that may be viewed by a user according to the user's predetermined

privileges on the user computer system. Therefore, it would have been obvious for one of

ordinary skill in the art at the time the invention was made to modify the Thorsen system

by including a database for storing object and associated information, an application

server controlled by software code in memory, access data application code being

responsive to the access criteria associated with the groups of data contained within a

version of an object and to predetermined privileges for allowing controlled access to

individual groups of data contained within the version of the object by an individual user

that was set up to be sent to a user computer an that may be viewed by a user

according to the user's predetermined privileges on the user computer system in order

to control access to data and providing different views of stored data objects depending

on different aspects of the stored objects or different access rights of a user.

Regarding to claim 2, Thorsen teaches all the claimed subject matters as

discussed in claim 1 and further discloses: *the access data application code enables the*

ability of a user to read the contents of the transferred version of the requested object that was

sent by the application server according to access privileges associated with the user (Col. 10,

line 42-Col. 11, line 5).

Regarding to claim 3, Thorsen teaches all the claimed subject matters as

discussed in claim 2, except *the access data application code includes the ability to modify*

the contents of version of the requested object. However, Thorsen teaches the structure of

an access node includes a control file that specifies a field to represent the relevant

access level for that node and a letter represents this field, for example: "r" means that

reading is allowed (Col. 10, lines 42-60). Thus, the field can be represented in different

predefined relevant access levels, which depends upon the access criteria such as:

modifying, deleting, or adding. Therefore, it would have been obvious for one of ordinary

skill in the art at the time the invention was made to modify the Thorsen control file in an

access structure to have a field that indicates the ability to modify the contents of the

requested object in order to manipulate the data if a user has the specified access

rights.

Regarding to claim 4, Thorsen teaches all the claimed subject matters as

discussed in claim 3, except *the ability to modify includes the ability to delete information*

contained in the version of the requested object. However, Thorsen teaches the structure of

an access node includes a control file that specifies a field to represent the relevant

access level for that node and a letter represents this field, for example: "r" means that

reading is allowed (Col. 10, lines 42-60). Thus, the field can be represented in different

predefined relevant access levels, which depends upon the access criteria such as:

modifying, deleting, or adding. Therefore, it would have been obvious for one of ordinary

skill in the art at the time the invention was made to modify the Thorsen control file in an

access structure to have a field that indicates the ability to delete information contained

in the requested object in order to manipulate the data if a user has the specified access

rights.

Regarding to claim 5, Thorsen teaches all the claimed subject matters as

discussed in claim 3, except *the ability to modify includes the ability to add data to the*

version of the requested object. However, Thorsen teaches the structure of an access

node includes a control file that specifies a field to represent the relevant access level

for that node and a letter represents this field, for example: "r" means that reading is

allowed (see col. 10, lines 42-60). Thus, the field can be represented in different

predefined relevant access levels, which depends upon the access criteria such as:

modifying, deleting, or adding. Therefore, it would have been obvious for one of ordinary

skill in the art at the time the invention was made to modify the Thorsen control file in an

access structure to have a field that indicates the ability to add information to the

requested object in order to manipulate the data if a user has the specified access

rights.

Regarding to claim 6, Thorsen teaches all the claimed subject matters as

discussed in claim 1, except *the access to the version of the object is determined by a*

business relationship to produce products and defined by the host according to the need of

information in the product chain, and wherein the transferred version of the object is

configured to reveal limited information according to a guest user's predetermined access

privileges. However, Thorsen teaches: the system to manage and access data of an

enterprise with different departments such as finance, production, sales and storage...

(Col. 1, lines 14-27) that leads to controlling access as an object of Thorsen system

(Col. 3, lines 8-22). This indicates a business relationship that has productions and the

need of information in the product chain, also the access right defined by the host. In

addition, at step 124 of FIG. 8, upon a user command (cmd=dir) all objects are copied to

or listed in an object list 128. Thereafter, in step 132 every object in the object list is

checked in respect of whether or not the user is permitted access to it. An object access

list 134 is thereby used as a check reference. If access right exists for an object, a copy

of or a reference to that object is input in a user list, step 136, and is communicated to

the user in step 138 by call 140 (Col. 11, line 34-Col. 12, line 11). This indicates the

transferred version of the object is configured to reveal limited information according to

a guest user's predetermined access privileges. Therefore, it would have been obvious

for one of ordinary skill in the art at the time the invention was made to modify the

Thorsen system to have a business relationship that determine the access to the

information in the product chain in order to exchange business data in a proper way.

Regarding to claim 7, Thorsen teaches a method for accessing data in a

computer-based data processing comprises: *storing an object, the object comprising*

distinguishable groups of data, each group of data having associated access criteria for access

to the groups of data (FIG. 3B, Col. 8, lines 43-56); *storing software code for controlling the*

operation of the CPU in memory (FIG. 1, Col. 7, lines 5-16). As shown in FIG. 3B,

Thorsen discloses a state of the art database 52, storing data in a number of tables 54

and being provided with specific data associations. Depending on a control file, the data

associations are rearranged; references or pointers to each of the selected data items

of the tables 54 are arranged and stored in a number of data access nodes 56 as *an*

application server. A client 58, for example an application program, communicates with

the access nodes 56 of the access structure and a new interface is provided between

the old database and the user (Col. 8, lines 42-52). This indicates the step of *controlling*

the access to the database using an application server. As shown in FIG. 8 is a flow chart for

implementing an object access control means or an object filter. The object filter is used

in conjunction with the access control to protect an object referred to by an access

node. In step 124, upon a user command (cmd=dir) all objects are copied to or listed in

an object list 128. Thereafter, in step 132 every object in the object list is checked in

respect of whether or not the user is permitted access to it. An object access list 134 is

thereby used as a check reference. If access right exists for an object, a copy of or a

reference to that object is input in a user list, step 136, and is communicated to the user

in step 138 by call 140 (Col. 11, line 66-Col. 12, line 11). As shown in FIG. 7 as a flow

chart of access control, an access node process is started and initialized in step 72, and

access node parameters concerning other nodes and objects referred to by the node

are read from a control file 74. In step 76 the access node is kept in a waiting condition,

waiting for incoming user calls 78. If a user call is received, the access node process

starts a subprocess in step 80 and sets a timer depending on the control file 82 for the

period the subprocess is allowed to exist. In step 84, the subprocess verifies the user,

depending on control file 86 containing information about accepted and permitted user

identities. The address and the identity of the user is polled in communication 88. If the

user is permitted and accepted, the user is logged in to the access node in step 104 and

106 and is allowed access to functions of the access node and objects encapsulated in

or referred to by the access node. Thereafter, further access to and communication of

data and references contained in the access node is controlled by means of an access

filter having certain access control parameters and allowing different users different

views of the access node, the access structure and the underlying data. In step 124 of

FIG. 8, upon a user command (cmd=dir) all objects are copied to or listed in an object

list 128. Thereafter, in step 132 every object in the object list is checked in respect of

whether or not the user is permitted access to it. An object access list 134 is thereby

used as a check reference. If access right exists for an object, a copy of or a reference

to that object is input in a user list, step 136, and is communicated to the user in step

138 by call 140 (Col. 11, line 34-Col. 12, line 11). This indicates the steps of *an*

application server, that is configured to set up a version of an object according to access

criteria; transferring a version of an object to a user in the form of a document file having the

version of the object and any associated documents request by a user contained therein; and

allowing controlled access to individual groups of data contained within the object by an

individual user according to the user's privileges in response to the access criteria associated

with the group of data contained within an object and to predetermined privileges. Therefore,

it would have been obvious for one of ordinary skill in the art at the time the invention

was made to modify the Thorsen method by including the steps of storing an object,

controlling the access to the database using an application server, transferring a version

of an object to a user and allowing controlled access to individual groups of data

contained within the version of the object by an individual user that may be viewed by a

user according to the user's predetermined privileges on the user computer system in

order to control access to data and providing different views of stored data objects

depending on different aspects of the stored objects or different access rights of a user.

Regarding to claim 8, Thorsen teaches all the claimed subject matters as

discussed in claim 7, and further discloses the steps of *receiving an object request by a*

requestor (FIG. 7, Col. 11, lines 41-46); *verifying the requestor's user privilege access*

criteria (FIG. 7, Col. 11, lines 49-53); and *transmitting a version of an object configured to*

reveal information contained with in the version of the object according to the requestor's user

privilege access criteria (FIG. 7, Col. 11, lines 53-65).

Regarding to claim 9, Thorsen teaches all the claimed subject matters as

discussed in claim 7, and further discloses the steps of *establishing a version of an object*

includes loading information into the version of an object into separate groups having

separate access privilege criteria (FIG. 2-3A; Col. 8, lines 12-34).

Regarding to claim 10, Thorsen teaches all the claimed subject matters as

discussed in claim 7, and further discloses the steps of *establishing privilege access*

criteria includes identifying the separate groups of information to which the user may access

for use in setting up a version of the object to be sent to the user in response to the user

request (Col. 11, lines 6-33).

Regarding to claim 11, Thorson teaches all the claimed subject matters as

discussed in claim 7, and further discloses the step of *verifying the requestor's user*

privilege access criteria includes extracting the requestor's user identification from the object

request (FIG. 7, Col. 11, lines 34-41); *verifying the requestor's user identification* (Col. 11,

lines 41-53) and *identifying the groups of data within the version of the object to which the*

requestor has access (Col. 11, lines 56-65).

Regarding to claim 12, Thorson teaches all the claimed subject matters as

discussed in claim 7, and further discloses the step of *transmitting a redacted version of*

an object by sending an electronic object to the requestor that contains the groups of

information to which the requestor has access to and that excludes groups of information

associated with an object to which the requestor does not have access (Col. 11, lines 56-65).

Response to Arguments

9.   Applicants' arguments with respect to claims 13-15 filed on 06/27/2002

have been fully considered but they are not persuasive.

Regarding to claims 13-15, claim 13 was amended to have *a computer readable*

*code means for identifying a user to have **limited** access to **information associated with** the*

*object and transmitting **a version of the requested object in the form of** a redacted document*

*that **masks information** according to the requestor's privilege access criteria*. Thorsen

teaches a system for controlling access to and associating data in an application

independent fashion. The Thorsen system enables data of different nature to be

handled in a conform way and for allowing different views as *the versions* of stored data

objects depending on different aspects of the stored objects or different access rights of

a user (Col. 3, lines 9-22). Thorsen teaches: access rights are checked on several

levels, for example, the address of the user application or client is first checked, and if

the address is known, the access rights of the client is then checked. Every object and

reference of an access node has an access list, which is polled before a client

command is executed. Thorsen further discloses access control parameters such as

read, write for constituting an access filter that is arranged to let different interested

parties or clients have their specific view of the stored object, object or references of the

access node (Col. 11, lines 6-33 and Col. 10, lines 56-60). As in FIG. 8 at step 124,

upon a user command (cmd=dir) all objects are copied to or listed in an object list 128.

Thereafter, in step 132 every object in the object list is checked in respect of whether or not the user is permitted access to it. An object access list 134 is thereby used as a check reference. If access right exists for an object, a copy of or a reference to that object is input in a user list, step 136, and is communicated to the user in step 138 by call 140 (Col. 12, lines 3-11). This indicates the *means for identifying a user to have limited access to information associated with the object and transmitting a version of the requested object in the form of a redacted document that masks information according to the requestor's privilege access criteria*. Thus, it is believed that amended claim 13 is not defined over the Thorsen prior art. In addition, claims 14-15 depend directly or indirectly upon claim 13 are also rejected as being anticipated by Thorsen as discussed in the office action.

Conclusion

9.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

10.   A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is

not mailed until after the end of the THREE-MONTH shortened statutory period, then

the shortened statutory period will expire on the date the advisory action is mailed, and

any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date

of the advisory action. In no event, however, will the statutory period for reply expire

later than SIX MONTHS from the date of this final action.

11.   Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Hung Pham whose telephone number is 703-605

4242. The examiner can normally be reached on Monday-Friday, 7:00 Am - 3:30 Pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, VU, KIM YEN can be reached on 703-305 4393. The fax phone numbers

for the organization where this application or proceeding is assigned are 703-746 7239

for regular communications and 703-746 7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305 3900.

Examiner: Hung Pham
July 8, 2002

HOSAIN T. ALAM
PRIMARY EXAMINER